By: Sachin Verma Contact.verma7@Gmail.com

FareIt Malware Analysis using static and dynamic method

What is FareIt?

This form of malware was discovered in 2012, but has continued modifying throughout the years to bypass anti-virus protection. It is an information stealer that targets FTP credentials, email passwords and browser stored passwords. During dynamic analysis, it is observed all of the above being performed after the malware disabled local security tools.

How it is spreading to the crowd?

The most recent Fareit malware threat is being distributed via a phishing attack. A phishing attack is an email with a malicious link or attachment, designed to make you click on those links/attachments. This most recent phishing attack includes malicious executable disguised as a DOC, XLS, ISO, PPT file attachment, which includes the malware. Once the user downloads the Attachment, their computer becomes infected and the malware scans for any credentials that may be of value. This may range from banking information, various account login credentials, administrative credentials, etc.

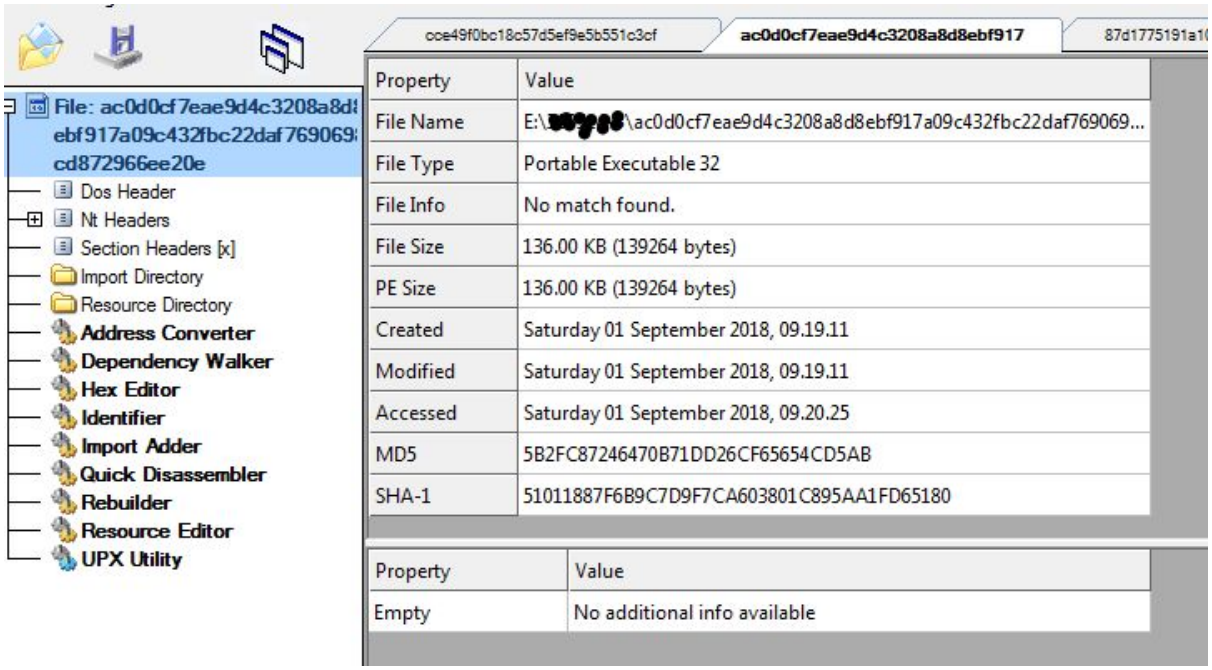
Spam email with an attachment *Attached Malicious Document file* *Fareit Malware*

Fareit Static Analysis:

SHA256: ac0d0cf7eae9d4c3208a8d8ebf917a09c432fbc22daf7690698cd872966ee20e

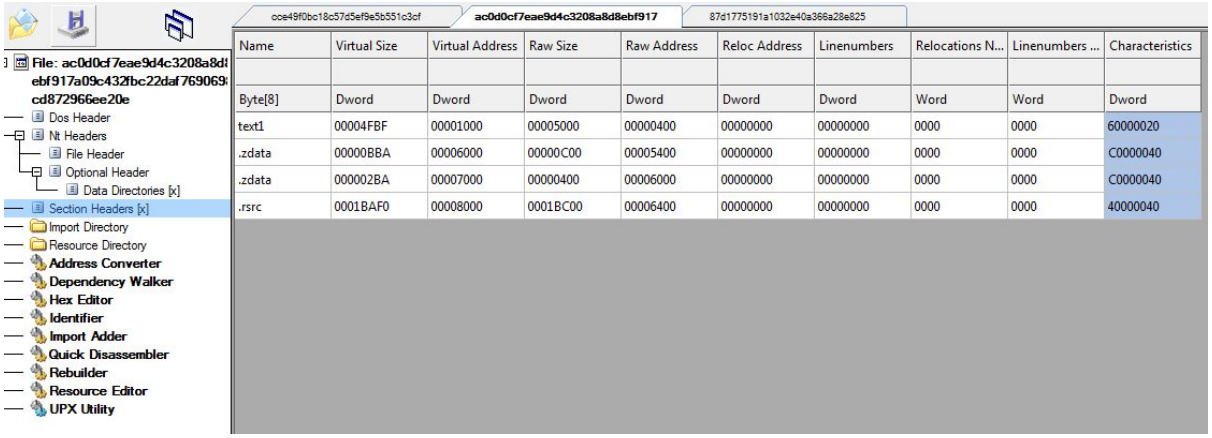
---

File General information:



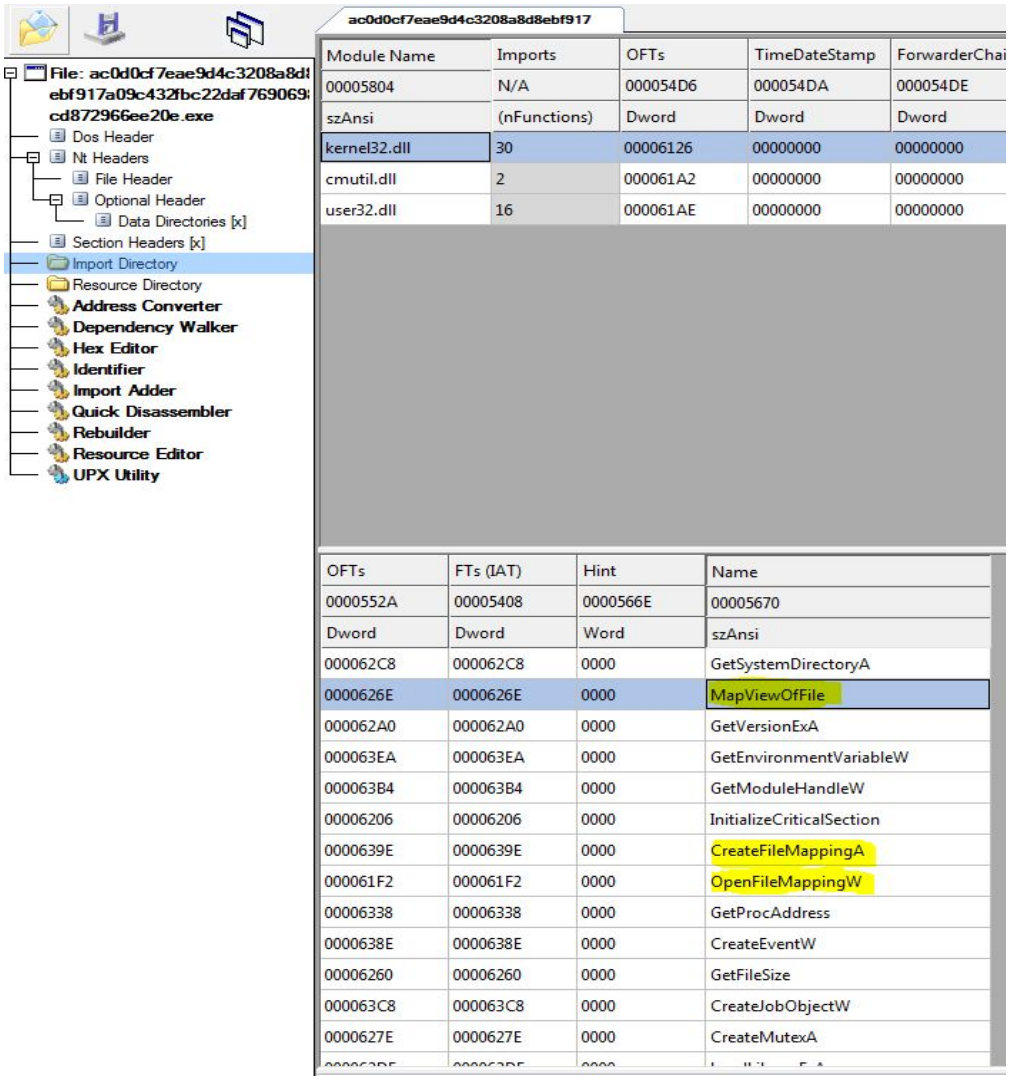
- No information related to Company Name, File Description, Legal Copyright, Product Version ext. (suspicious)

File Section headers:



- Odd looking Non-Standard sections name: text1, odata, .wdata (suspicious)

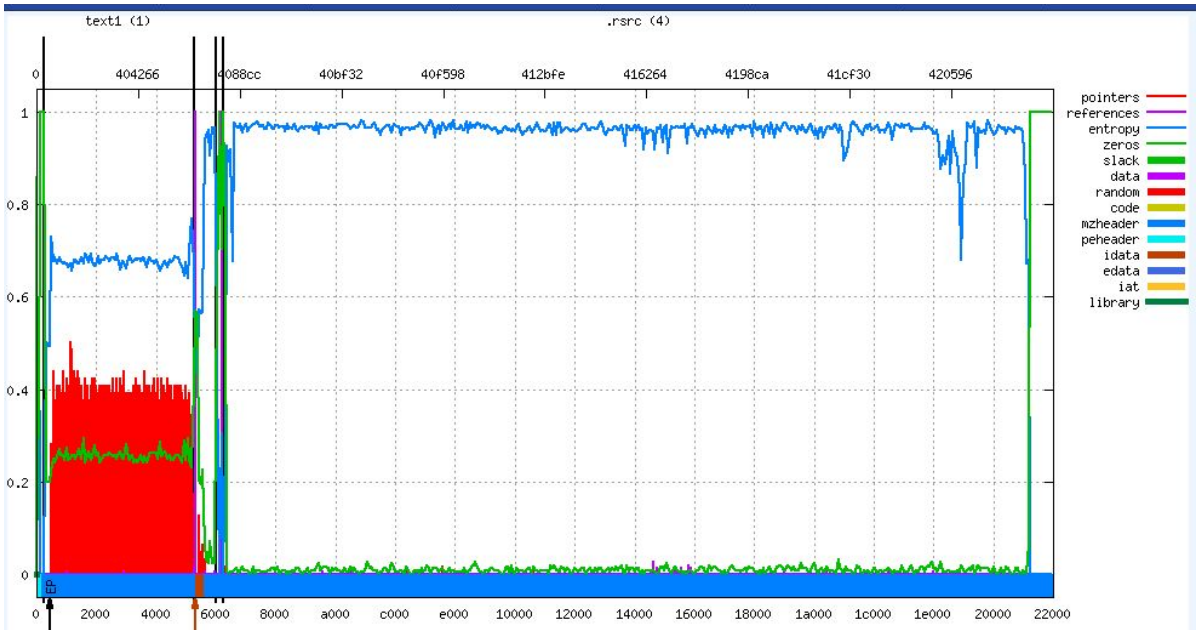
File Import Directory:



- It is importing some functions related to File mapping.

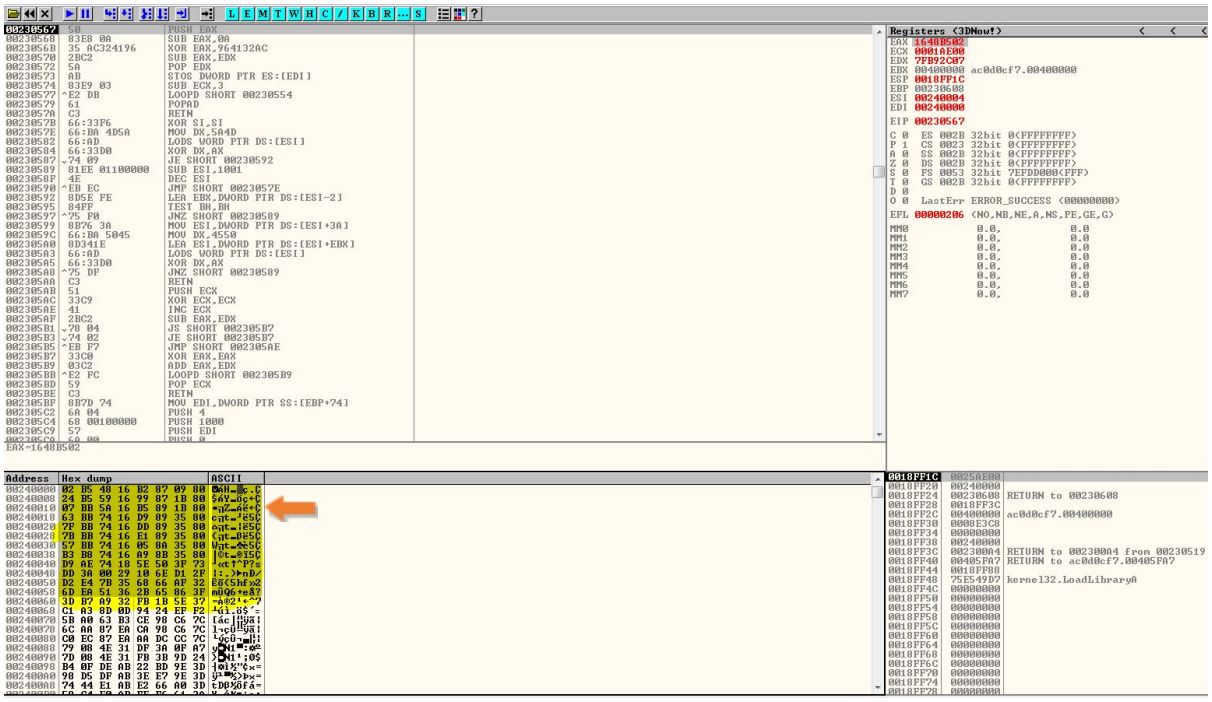
MapViewOfFile: Maps a view of a file mapping into the address space of the calling process.
CreateFileMappingA: Creates or opens a named or unnamed file mapping object for a specified file.
OpenFileMappingW: Opens a named file mapping object.

File Heu:

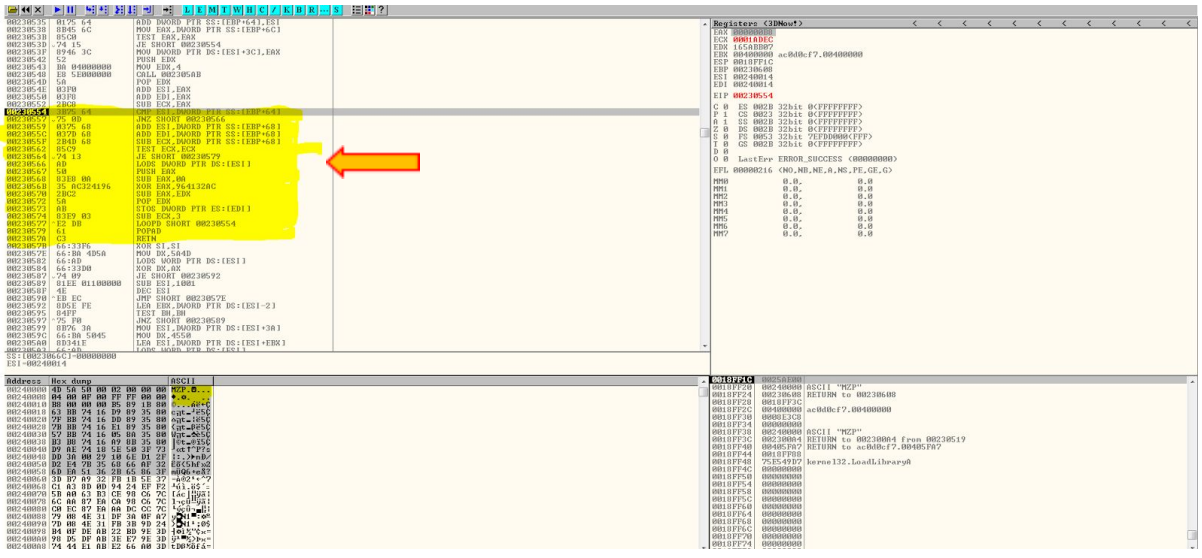


- File's Resource section is very large and dens, probably having encrypted data

I have opened same file in ollyDbg and found that file is putting encrypted data to Hex Dump



Now the data will get decrypted by a decryption loop:



Here is the decryption loop code:

```
002B0554   3B75 64        CMP ESI,DWORD PTR SS:[EBP+64]
002B0557   75 0D          JNZ SHORT 002B0566
002B0559   0375 68        ADD ESI,DWORD PTR SS:[EBP+68]
002B055C   037D 68        ADD EDI,DWORD PTR SS:[EBP+68]
002B055F   2B4D 68        SUB ECX,DWORD PTR SS:[EBP+68]
```

```
002B0562   85C9            TEST ECX,ECX
002B0564   74 13          JE SHORT 002B0579
002B0566   AD             LODS DWORD PTR DS:[ESI]
002B0567   50             PUSH EAX
002B0568   83E8 0A        SUB EAX,0A
002B056B   35 AC324196     XOR EAX,964132AC
002B0570   2BC2           SUB EAX,EDX
002B0572   5A             POP EDX
002B0573   AB             STOS DWORD PTR ES:[EDI]
002B0574   83E9 03        SUB ECX,3
002B0577  ^E2 DB          LOOPD SHORT 002B0554
002B0579   61             POPAD
```

It decrypt's an executable file SHA 1: bb5d9b8aee93ef92cea52849b17f57bb4e3c0306

Behavior of the base file is suspicious itself, which is dropping another executable into the memory dump.

FareIt Dynamic analysis:

I have executed the file into safe environment and found some results:

After execution I have gathered data of file's Properties -> Strings -> strings and found some suspicious looking string form there:

- String Related to Passwords, Hostname

```
30  ]]]
31  HostName
32  PortNumber
33  UserName
34  Password
```

- Strings related to embedding a executable file in tempbuffer.dat

```
%APPDATA%\.purple\accounts.xml
%TEMP%\tempbuffer.dat
MZP
This program must be run under Win32
CODE
`DATA
BSS
.idata
.reloc
P.rsrc
.idata
.reloc
P.rsrc
Char
Byte
```

- Found Functions related to Find first file, Excessive number of FindFirstFile calls (suspicious)

```
FindFirstFileW
FindNextFileW
```

- Found functions related to Hashing. (suspicious)

```
CryptAcquireContextA
CryptCreateHash
CryptHashData
CryptGetHashParam
CryptDestroyHash
CryptReleaseContext
```

The CryptCreateHash function initiates the hashing of a stream of data.

- Function to get keyboard layout.

```
GetKeyboardLayoutList
```

- Having Strings related to Browsers, email applications, Chat applications.

```
MozillaBased
```

```
InternetExplorer
```

```
Server
Outlook
```

```
Skype
Telegram
D877F783D5*,map*
%appdata%\Telegram Desktop\tdata\
```

- Having Strings Related to bit coin wallet related keywords.

```
%APPDATA%\
wallet.dat
\wallet.dat
electrum.dat
\electrum.dat
.wallet
\.wallet
%APPDATA%\MultiBitHD
mbhd.wallet.aes
\MultiBitHD\
\mbhd.wallet.aes
\mbhd.checkpoints
mbhd.checkpoints
\mbhd.spvchain
mbhd.spvchain
\mbhd.yaml
mbhd.yaml
wallet_path
Software\monero-project\monero-core
\Monero\
.address.txt
.keys
strDataDir
Software\Bitcoin\Bitcoin-Qt
\BitcoinBitcoinQT\wallet.dat
CPU Model:
jjjjjjjj
UTC+
Ajj
Coins
Coins\Electrum
%appdata%\Electrum\wallets\
```

- Having some base64 encoded strings:

Before decryption

```
U29mdHdhcmVcTWljcm9zb2Z0XFdpbmRvd3NcQ3VycmVudFZlcnNpb25cVW5pbnN0YWxs
RGlzcGxheU5hbWU=
U29mdHdhcmVcTWljcm9zb2Z0XFdpbmRvd3NcQ3VycmVudFZlcnNpb25cVW5pbnN0YWxsXA==
RGlzcGxheVZlcnNpb24=
```

After decryption

```
Software\Microsoft\Windows\CurrentVersion\UninstallDisplayName
Software\Microsoft\Windows\CurrentVersion\Uninstall\
```

- Got a suspicious URI(which is malware repo categorized) (malicious connection)

```
system-check.xyz/index.php
```

- Probably saving all credentials to below file.

```
919  PasswordsList.txt
```

- Probably creating a JSON object to post data through the above URI

```
923  ip-api.com/json
924  "query":"
925  "countryCode":"
926  ip.txt
927  System.txt
928  reportdata=<info
929  </info
930  <pwds
```

From the above Strings, it does have a credential stealing + bitcoin related data stealing properties.
Those are same as Fareit malware family.

Because of its anti-analysis feature I am not able to execute the malware to its full potential.
But above analysis is enough to prove sample as a Fareit malware family.